UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,913	04/16/2004	Jian Zhang	CN920030004US1	8907

67158 7590 11/14/2007

SHIMOKAJI & ASSOCIATES, P.C.
8911 RESEARCH DRIVE
IRVINE, CA 92618

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
11/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/825,913	ZHANG ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-9,11,13,20-22 and 25-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-9,11,13,20-22 and 25-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 23 August 2007 has been noted and made of record.

2. Claims 1-3, 6-9, 11, 13, 20-22, and 25-27 have been presented for examination.

3. Claims 4, 5, 10, 12, 14-19, 23, and 24 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's amendment, see claim 11, have been fully considered and are persuasive. The objection of claim 11 has been withdrawn.

5. Applicant's amendment, see claim 20, have been fully considered and are persuasive. The 35 U.S.C. 101 rejection of claims 20-27 has been withdrawn.

6. Applicant's arguments with respect to the prior art rejections of claims 1-3, 6-9, 11, 13, 20-22, and 25-27 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Objections

7. Claim 1 is objected to because it recites "the digital asset server receiver requests from the digital asset client." For the sake of examination, the Examiner will construe the limitation to be "the digital asset server receiving requests from the digital asset client." Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-3, 6-9, 12, 13, 20-22, 25, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0073047 A1 to Morrison,

hereinafter Morrison, in view of U.S. Patent Application Publication No. 2003/0204515 A1 to Shadmon et al, hereinafter Shadmon, and further in view of U.S. Patent No. 7,095,850 B1 to McGrew, hereinafter McGrew.

10. As per claims 1 and 20, Morrison teaches a method and a program product for generating hierarchical keys of digital assets, encrypting the digital assets in a digital asset server, and utilizing the keys of the digital assets and the encrypted digital assets in an associated digital asset client, comprising the steps of:

arranging the digital assets in the digital asset server (paragraph 0017, i.e. server system maintains all files);

encrypting corresponding digital assets in the digital asset server using the computed keys (paragraphs 0017, 0023, i.e. maintaining encrypted files at the server);

requesting an encrypted digital asset at the digital asset client (paragraph 0022, i.e. client initiates transaction for encrypted file), and determining if a key for the requested encrypted digital asset is present on the digital asset client (Figure 4 [block 200], paragraph 0022);

if the digital asset key is not present on the digital asset client, the digital asset client requesting the digital asset key from the digital asset server (paragraph 0015, i.e. requesting the key indicates payment for access to the encrypted file);

the digital asset server receiver requests from the digital asset client, and thereafter transmits a digital asset key, if requested (Figure 4 [step 204], paragraph 0024, i.e. storing a portion of the encryption key in a cookie of the client system), and a requested encrypted digital asset from the digital asset server to the associated digital asset client (Figures 2 [block 22], 3 [block 100], paragraphs 0016, 0024, i.e. selecting a file to be downloaded); and

receiving the key (Figure 4 [blocks 204, 210], paragraphs 0022, 0023) and the encrypted digital asset from the digital asset server at the digital asset client (Figure 4 [block 208], paragraph 0024) and decrypting the encrypted digital asset utilizing the key (paragraph 0024).

11. Morrison does not teach wherein the digital assets are stored as at least one tree structure, a root node of the tree structure representing a complete set of the digital assets, other group nodes representing sub-sets in each level of the digital assets respectively, and the nodes in the lowest level being leaf nodes; randomly generating a key of the root node in the digital asset server; and starting with the key of the root node, using the key of a father node to compute level by level computed keys of its child nodes through to leaf nodes using a one way function, in the digital asset server.

12. Shadman teaches organizing data in a tree structure, wherein the root node of the tree represents all assets (Figures 1, 2, 3, 6, 7, 10-13, paragraphs 0003, 0056, 0057, 0064).

13. It would have been obvious to one of ordinary skill in the art at the time the invention was made to store the assets in at least one tree structure, a root node of the tree structure representing a complete set of the digital assets, other group nodes representing sub-sets in each level of the digital assets respectively, and the nodes in the lowest level being leaf nodes, since Shaman shows that it is well known to organize data in a tree structure, and that incorporating the tree structure into Morrison yields the predictable result of organizing data in a simple hierarchical manner. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

14. McGrew teaches randomly generating a key of the root node in the digital asset server (column 7, line 22 to column 8, line 26, column 12, lines 14-23);

starting with the key of the root node, using the key of a father node to compute level by level computed keys of its child nodes through to leaf nodes using a one way function, in the digital asset server (column 7, line 22 to column 8, line 26, column 12, lines 14-23).

15. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the key of the father node to compute the key of the child node, since McGrew states at column 5, lines 43-48 that the key updating method can efficiently generate one or more keys that are applicable to ciphers that are used in multicast and group settings.

16. Regarding claims 2 and 21, McGrew teaches computing different keys for two nodes having the same father node (Figures 7A, 7B, column 12, lines 3-48).

17. Regarding claims 3 and 22, McGrew teaches computing different keys for child nodes having the same father node (Figures 7A, 7B, column 12, lines 3-48).

18. With respect to claims 6, 12, and 25, Morrison teaches encrypting the corresponding digital assets using at least a part of the keys (paragraphs 0017, 0023, i.e. maintaining encrypted files at the server).

19. Concerning claims 7, 13, and 26, Morrison teaches encrypting the digital assets using a cipher and encrypting the cipher using at least a part of the generated node keys (paragraph 0017, i.e. DES).

20. Regarding claims 8 and 27, Morrison teaches wherein the digital assets are chosen from the group consisting of video, audio and text materials (paragraph 0016, i.e. files for download from Web sites include video, audio and textual materials).

21. As per claim 9, Morrison teaches an apparatus and a server for managing digital assets and hierarchical keys of the digital assets, comprising a digital asset server and a digital asset client:

said digital asset se rver comprising a central processor unit, a bus, and memory (paragraph 0017, i.e. server system maintains all files), and further comprising:

(d) an encrypting unit for encrypting the corresponding digital assets by using at least a part of the keys (paragraphs 0017, 0023, i.e. maintaining encrypted files at the server); and

said digital asset client comprising a central processor unit, a bus and memory and further comprising:

(a) a second computing unit for requesting an encrypted digital asset from the digital asset server (paragraph 0022, i.e. client initiates transaction for encrypted file), searching for node keys stored on the digital asset client for the requested digital asset (Figure 4 [block 200], paragraph 0022); and

(b) a decrypting unit for decrypting the digital assets contained in all nodes by using the computed node keys of all nodes of the requested digital assets (paragraph 0024).

22. Morrison does not teach (a) key tree management unit for arranging the digital assets as at least one tree structure for management, a root node of the tree structure representing the complete set of the digital assets, other group nodes representing sub-sets in each level of the

digital assets respectively, and the nodes in the lowest level being leaf nodes, said apparatus further comprises: (b) a root node key generating unit for generating the key of the rood node; and (c) a first computing unit for starting with the key of the root node, computing level by level the keys of its child nodes according to a predetermined one-way function, through to leaf nodes.

23. Shadman teaches organizing data in a tree structure, wherein the root node of the tree represents all assets (Figures 1, 2, 3, 6, 7, 10-13, paragraphs 0003, 0056, 0057, 0064).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to store the assets in at least one tree structure, a root node of the tree structure representing a complete set of the digital assets, other group nodes representing sub-sets in each level of the digital assets respectively, and the nodes in the lowest level being leaf nodes, since Shaman shows that it is well known to organize data in a tree structure, and that incorporating the tree structure into Morrison yields the predictable result of organizing data in a simple hierarchical manner. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

25. McGrew teaches randomly generating a key of the root node in the digital asset server (column 7, line 22 to column 8, line 26, column 12, lines 14-23);

starting with the key of the root node, using the key of a father node to compute level by level computed keys of its child nodes through to leaf nodes using a one way function, in the digital asset server (column 7, line 22 to column 8, line 26, column 12, lines 14-23).

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the key of the father node to compute the key of the child node, since McGrew states at column 5, lines 43-48 that the key updating method can efficiently generate one or more keys that are applicable to ciphers that are used in multicast and group settings.

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

28. The following patents are cited to further show the state of the art with respect to content distribution, such as:

United States Patent Application Publication No. 2004/0054681 A1 to Pitts, which is cited to show facilitating access to remote files.

United States Patent No. 7,240,365 B2 to de Jong et al., which is cited to show repositing for digital content access control.

United States Patent Application Publication No. 2004/0073903 A1 to Melchione, which is cited to show providing access to software over a network via keys.

United States Patent Application Publication No. 2005/0119967 A1 to Ishiguro et al., which is cited to show distributing licenses that are stored hierarchically.

United States Patent Application Publication No. 2005/0060334 A1 to Kawamoto et al., which is cited to show storing keys related to media in a hierarchical manner.

29. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

30. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

31. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

32. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

33. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf